Low Cost Reliable, Damage Tolerant Intelligent Distributed Control

Samuel M. Smith Ph.D.and Kevin White,

Adept Systems Incorporated

21271 Waycross Drive
Boca Raton, Florida 33428
561-487-6894 (voice) 561-487-6894 (fax)
adept@adeptsystemsinc.com (email)

and

Stanley E. Dunn, Ph.D

Ocean Engineeing Department

Florida Atlantic University
101 Ocean Boulevard
Dania Beach, Florida, 33004
954-924-7000
sdunn@oe.fau.edu

Abstract: The U. S. Navy is continuing in its effort to develop the technology that will allow it to deploy highly automated ships. The goal is to achieve increased reliability and afforability through significant manpower reductions in engineering, damage control, ship suport, and surge watch standing. Recent advances in automation technolgy support the believe that these improvements can be achieved through intelligent automation and the use of component level intelligent distributed control systems (CLIDCS). This paper describes recent work to produce the capability in CLIDCS for survivable, self-healing LonTalk control networks for shipboard automation.

1 PROJECT BACKGROUND

Adept System Inc. (ASI) was founded in 1994 for the purpose applying the expertise of the founders with the LonTalk protocol to commercial applications primarily through consulting and software development. As ASI developed for Echelon Corp. the C Reference Implementation of the LonTalk Protocol. This is now the basis for the EIA 709 open specification for the LonTalk Protocol. Subsequently ASI has developed proprietary higher performance implementations of the LonTalk protocol including a port to x86 processors. ASI has also developed for the Navy, control system software for a Land Based Demo of a chill water system employing LonTalk and a hardware in the loop damage simulation of sensors and actuators on a LonTalk Network.

The Office of Naval Research funded Florida Atlantic University to do a feasibility study on the use of LonTalk for survivable networks. The basic idea was to see if topologies and self-healing concepts currently used in expensive high end networking systems could be cost effectively applied to less expensive component level networks. Specifically this study was to see if the built in features of LonTalk and associated commercial off the shelf (COTS) support tools would enable survivable network topologies similar to that employed by other network protocols such as TCP/IP. The principle driver for the Navy was to leverage low cost COTS open distributed control network technology for shipboard automation. The feasibility study was successful in showing that LonTalk routers could be employed in a scalable reconfigurable topology consisting of a partial mesh of rings. However the study was not successful in the sense that it could not find COTS network management software tools that supported such a topology. The FAU work built a minimal network of 3 rings. Healing consisted of merely turning on one of the routers as a repeater. This was called a dependable topology with network fragment healing. The results of this work including the example source code were published in a FAU Technical Report and a couple of papers.[FAU 98][Smith 97][Smith 98].

The principle finding was that although the topology was feasible it was not practically implementable for shipboard automation because no COTS network management tools were available that supported automatic installation and configuration of a partial mesh of rings and more sophisticated rerouting algorithms were needed. The Navy however expressed interest in solving this problem by funding development of commercializable network management tools and rerouting algorithms for this survivable LonTalk Network Topology. The Navy's principle concern and requirement was that these tools be commercially supported.

Due to the expertise and experience of ASI and its founders, ASI was tasked to develop network management tools based on the ASI's high performance implementation of the LonTalk Protocol that supported the partial mesh of rings topology. ASI is also investing a considerable proprietary component of its LonTalk implementation as the basis for the network management tools. ASI's LonTalk stack brings significant usability and cross platform features not available elsewhere.

The principle goal has been to develop a set of automated network management and installation software tools for LonTalk based CLIDCS that support dependable topologies and self-healing. The tools are actually a library of functions with an application programmer's interface (API). Using these tools, a basic network management software application would then be developed. The network management software would include a set of configuration functions that would take a network control system design that employs a dependable topology and install the appropriate network bindings.

2 TECHNICAL BACKGROUND

2.1 Problem

A standardized general toolset of the associated hardware and software is being developed, documented, and commercially supported. The approach is being refined and extended to easily support 1000's of nodes. The idea is to leverage the substantial commercial market investment in LonTalk technology such as, transceivers, node, sensors, actuators, and routers by developing a software tool set that directly supports self-healing networks. This reduces the risk to the Navy in that a protocol and base line support systems do not have to be developed from scratch to meet Navy needs for more survivable networks but only enhancements to an existing full featured standard must be developed.

Current advanced Navy ships may only have a few hundred total control points attached to automatic control or monitoring equipment. For significant manning reductions to occur the number of control points will have to increase by at least one order of magnitude to thousands of control points and maybe 2 orders of magnitude to tens of thousands of control points. While the current LonTalk protocol and associated network management tools easily accommodate such large numbers of nodes in static networks, current COTS LonTalk network management software does not provide configuration support for multiply interconnected rings. This lack of support meant that for the test network the initial network configuration and installation had to be done manually. Manual configuration, installation, and management of thousands of nodes would be impractical. In order to be cost effective, the design, configuration, installation, management, modification, and maintenance of large distributed control networks must be automated.

2.2 Topology

COTS LonTalk nodes, transceivers, and routers can be configured into a scalable dependable topology consisting of a partial mesh of interconnected rings. Each ring is a subnet of nodes. A ring is inherently resistant to single point failures due to opens in the network wiring. Physical layer repeaters within the rings provide isolation due to shorts. The rings can have redundant media connecting the nodes in the ring further increasing reliability. The rings are interconnected with routers. The routers provide both physical isolation and traffic partitioning. Any ring can be connected to a number of other rings and redundant routers can connect any two rings. This topology is diagrammed in Figure 2.1 below.

a) This dependable topology provides a flexible, configurable, design trade-off between cost, performance, and survivability. The parameters are the number of nodes in each ring, the number of interconnects between rings, and the arrangement of interconnects between rings. For lower cost systems the number of nodes in each ring is high and the number of rings and interconnects between rings is low. This has a lower

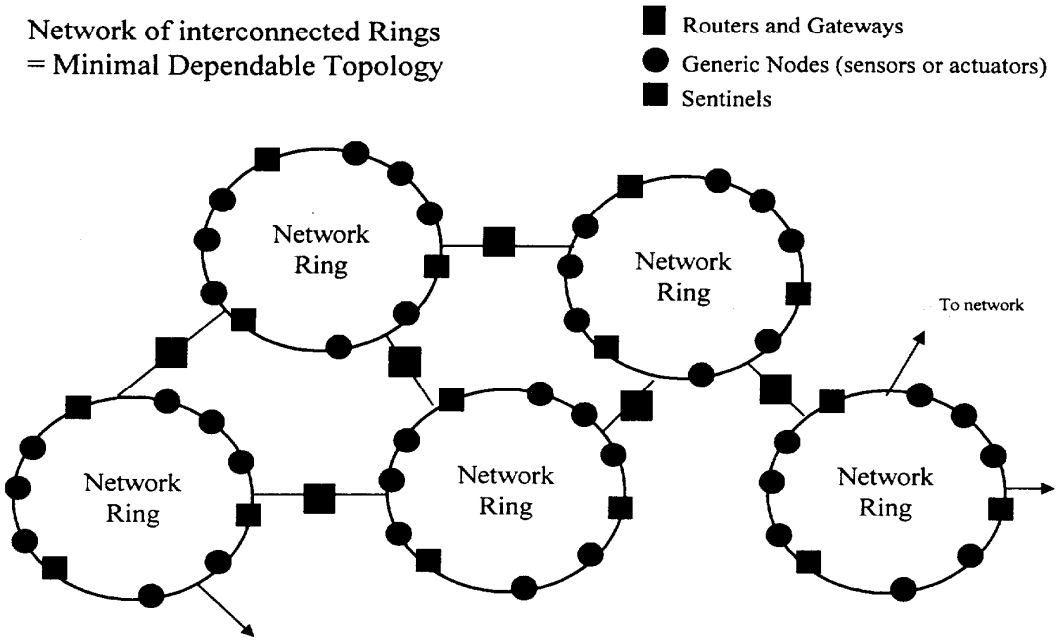

Figure 2.1 Scalable Dependable Topology

degree of redundancy but is still dependable and survivable. For highly survivable systems the number of nodes in a ring is low and the number of rings and interconnects between rings is high. This has a higher cost. For a given cost one can design for the most survivable network or vice-versa.

b) A system of Sentinel nodes with appropriate software can self-heal the network in the event of multiple point failures by reconfiguring the routers. Multiple failures of the network within a ring can produce "network fragments" that are cut off from the rest of the ring. The fragments can be reconnected or "healed" by rerouting traffic through neighboring rings.

c) The sentinel nodes can provide detection and reporting of failures or health monitoring of the network and nodes.

d) The degree of "intelligence" in the sentinel nodes and the sophistication of the reconfiguration algorithms provides another configuration design parameter that also governs cost, performance, and survivability.

e) An approach was developed for mapping and simulating a given application on a generic test network than can provide an estimate of network performance with different arrangements of the topology

In general, current commercially available approaches to component level distributed control networks do not support self-healing of network fragments in the event of multiple failures. Even networks with redundant media still have a common mode failure since the redundant media becomes co-located at each node connection. A damage event that disables the node could simultaneously disable both network connections. A second such event at another node would create a network fragment that cuts off the undamaged nodes on that network fragment from the rest of the ring. The only way to "heal" this level of damage is to provide an alternative path that reconnects the fragments.

2.3 Routing

In LonTalk channels are physically isolated media and subnets are logically distinct address groups. Typically each channel is given a unique subnet number. However, a Subnet can span multiple channels and multiple Subnets can exist on a single channel. Configured Routers partition traffic based on subnet address and physically isolate the two channels that are connected to each side of the Router. Traffic isolation only makes sense between channels with mutually exclusive Subnet numbers.

The current LonTalk router API only supports a static simple tree network. By static it is meant that the configuration is determined a priori and does not change. So any configuration algorithms can be executed once and set the configuration tables on the routers in the network. By simple tree network it is meant that there is only one path between any two nodes. There are no loops or multiple paths between nodes. By path it is meant the sequence of Channels/Subnets that a packet must traverse to get from one node to another. Redundant routers, however, are allowed between two channels. This is not a multiple path but a duplicate path. The duplicate detection mechanism in LonTalk filters out the redundant packets generated by the redundant routers. The reason this is not allowed is because the algorithm used by Echelon to configure the routing tables is a simple tree search. The algorithm starts at a Subnet and then follows every path connected to the Channel associated wit the Subnet. All the subnets found on the far side of a Router constitute the routing table for the near side of the router and vice versa. A loop or multiple path would cause the search algorithm to never terminate since it would keep returning to the same subnet.

The new API will be capable of supporting configurations like that shown in Figure 2.2 below. That means the database must allow the installation of routers in a looping configuration with one of the routers off-line under normal operation. The routing tables should be properly configured to support the required network variable bindings. The API and database must also store the proper re-configuration needed in the case of a network fragment or a least enough information to parametrize the Sentinel reconfiguration algorithms. For the nearest neighbor case the reconfigurations are straightforward. For example Figure 2.3 shows the reconfiguration given two network fragments in Channel A. Given that Node 3 must communicate with Node 1 all the Router tables must pass Subnet 1 traffic both ways. Similar reconfigurations would apply in the case of fragments in Channels B and C.

The API should be able to generate a subset of the network "image" for the Sentinel nodes. This image would contain the initial "healthy" configuration of the Nodes, Sentinels, and Routers in each Sentinel's ring and the Sentinels in each neighboring ring. In addition each Sentinel should be given the router configurations needed to heal fragments within its own ring and its nearest neighbor rings. The objective is to automate as much as possible the set-up and configuration of dependable topology and self-healing LonTalk networks.

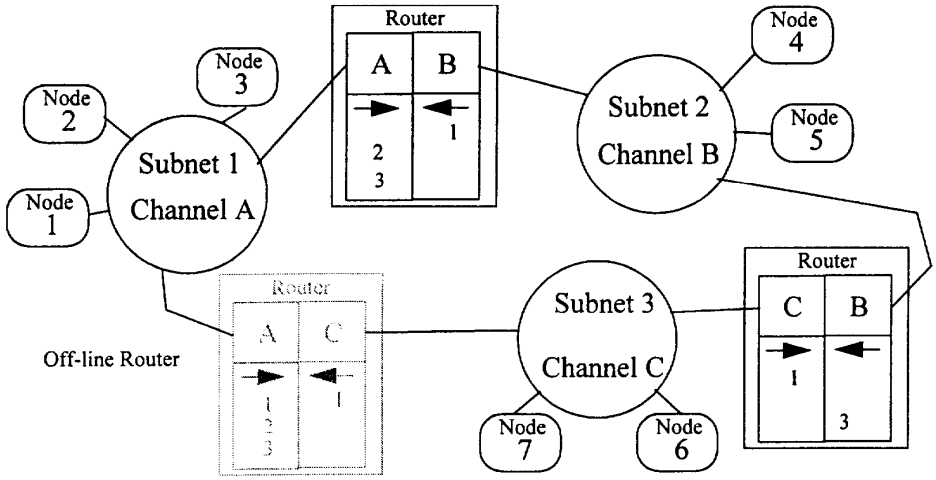

Figure 2.2 Initial configuration of network with off-line Router A/C and no fragments.

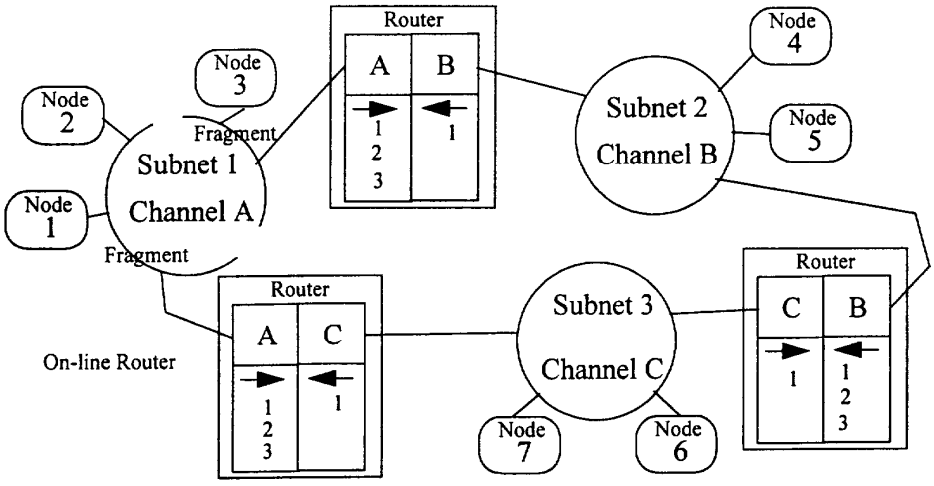

Figure 2.3 Configuration of network with network fragment in Channel A and on-line Router A/C

3 ADDITIONAL TECHNOLOGY BEING DEVELOPED

3.1 Advanced Rerouting Algorithm Investigation

The project's primary focus to develop network management tools and support for nearest neighbor rerouting. Implementation of more complex rerouting algorithms requires some preliminary research investigation and simulation before commercial implementation is cost effective. The work is investigating methods for recursively routing through neighbors of neighbors. This requires sophisticated search algorithms to find, rank, and select alternative paths. An intelligent agent approach is appropriate to the distributed nature of the networks and is inherently more survivable. The overriding consideration is cost effectiveness, that is, addressing the question of how much more survivable is the network and at what increase in cost and complexity when more advanced approaches are used.

3.2 Combined Router/Sentinel Node

The Sentinel nodes contain all the "smarts" as far as the self healing algorithm's are concerned. The Sentinels provide health monitoring and logging of node status and detection of single point failures in addition to reconfiguring routers to heal fragments. However a Sentinel can do little to reconfigure or heal a fragment unless a router also is connected to the Sentinel's fragment. It makes sense from a packaging point of view to combine sentinel and router function into a single node. The commercially available off the shelf LonTalk Routers do no provide support for reprogramming their functionality. Consequently there is no way to combine sentinel and router function using COTS routers. An intermediate solution is to combine some Sentinel nodes and Router nodes in the same housing.

4. Demonstration

An additional component of this effort in involved in the demonstration of these intelligent control networks. The intent is to select a size of project that is meaningful in its scope yet not so complex and difficult to implement that it proves too expensive and impractical. To meet these requirements a Yard Patrol vessel has been selected out of the fleet that is employed at the United States Naval Academy for the training of midshipmen in ship handling. The YP is something over 120 feet in length, is twin screwed, and is configured in all of its systems to mimic an actual naval vessel. For example, there is an engine room control station in the same fashion that a full size ship has an engine room control station. Thus, the YP has the array of systems that would be configured for intelligent control in a full size naval vessel yet the cost of modifying the vessel and maintaining the vessel is within reason.

Another feature of this aspect of the program is the inclusion of selected naval midshipmen in the design of systems controls, installation of the control systems, as well as the use and evaluation of the automation systems. It is thought that these young future naval officers, with their high degree of computer familiarity are ideal subjects on which to test these systems in this early phase of the demonstration and evlauation process.

5. Summary

An ongoing effort is underway to adapt and enhance commercially available intelligent distributed control technology to the needs of the Navy. Building on previous experience with intelligent distributed controls, a program is underway that will evaluated and demonstrate through actual installed systems the viability of robust, self healing intelligent control systems on navy vessels. The tools being developed in this effort will lead directly into capabilities to design and install robust CLIDCS based systems in production Navy ships of the future.

4 REFERENCES

FAU 98 Dependable Network Topologies With Network Fragment Healing For C.L.I.D.C.S. For Naval Shipboard Automation, Final Report, May 1998 by S. Smith, K. White, S. Dunn, and S. Gupta

Smith 97 Smith, S.M., Dunn, S. E., White, K., & Marquis, L, "Component Level Intelligent Distributed Control for Ship Automation", International Maritime Defence Exhibition and Conference, Greenwich UK, October 7-10, 1997

Smith 98 Smith, S.M., Dunn, S. E., & White, K. "Shipboard Automation using Component Component Level Intelligent Distributed Control and Sensing Systems",ASNE Symposium on 21st Century Combatant Technology, Pascagoula MS, 27-30 January, 1998 pp. 236-244.